

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

**BALDINO’S LOCK & KEY SERVICE,  
INC., et al.,**

Plaintiffs,

v.

**GOOGLE LLC, et al.,**

Defendants.

Case No. 1:16-cv-02360 (TNM)

**MEMORANDUM OPINION**

In 2014, Baldino’s Lock & Key Service, Inc. (Baldino’s) brought suit against Google LLC and two online directories in the United States District Court for the Eastern District of Virginia. The suit alleged that the defendants had violated the Lanham Act and the Racketeer Influenced and Corrupt Organizations Act (RICO) by listing numerous scam locksmiths on their websites, thus harming the plaintiff’s business. *Baldino’s Lock & Key Serv., Inc. v. Google, Inc.*, 88 F. Supp. 3d 543, 546 (E.D. Va. 2015). The district court dismissed the case, reasoning that the defendants enjoyed immunity under the Communications Decency Act (CDA) as providers of an “interactive computer service” against a suit trying to hold them “liable for content originating with a third-party information content provider,” and that each count independently failed to state a claim. *Id.* at 546-47. The Fourth Circuit affirmed the district court’s decision without mention of the CDA, since Baldino’s had abandoned all RICO claims on appeal, and the Lanham Act claim failed because the district court had “correctly determined” that the “locksmiths who generated the information that appeared on Defendants’ websites are solely responsible for

making any faulty or misleading representations.” *Baldino’s Lock & Key Serv., Inc. v. Google Inc.*, 624 F. App’x 81, 82 (4th Cir. 2015).

The instant suit relies on similar factual allegations, but with a slightly different array of defendants, plaintiffs, and claims. This time, the suit names search engine providers Google, Yahoo! Inc., and Microsoft Corporation (the Providers) as defendants. Baldino’s is now the lead plaintiff in a putative class action, joined by licensed locksmiths from around the country (the Locksmiths), who allege that the Providers are burying legitimate locksmiths under scam locksmiths in search results on the Providers’ websites, forcing legitimate locksmiths to pay for premium advertising slots or face the reality of an eroding customer base. First Am. Compl. 8-9 (Compl.). The Locksmiths allege violations of the Lanham Act and the Sherman Antitrust Act, and assert five state law causes of action. In an effort to avoid a repeat outcome, the Locksmiths emphasize that the Providers create mapping information based on scam locksmiths’ allegedly false location claims, contending that the Providers have thus created original content not immunized by the CDA. Nonetheless, the Providers move to dismiss, claiming that they enjoy immunity under the CDA for seven of the eight counts, that all counts independently fail to state a claim, and that claim preclusion bars Baldino’s allegations against Google. Defs.’ Mot. Dismiss i, 4-24. For the reasons that follow, I conclude that CDA immunity bars all of the Locksmiths’ claims except for breach of contract, and that the Locksmiths have failed to adequately plead that claim. Accordingly, all counts will be dismissed.

## I. BACKGROUND

The Locksmiths allege that the Providers control 90% of “organic and map internet search[es] originating in the United States.”<sup>1</sup> Compl. 8. “‘Organic’ search results are the unpaid list of links displayed . . . ordinarily ranked by their respective ‘relevanc[e]’ to a consumer’s search term.” *Id.* According to the complaint, the Providers “knowingly and deliberately flood organic search results [for] queries such as ‘locksmith’ . . . with scam locksmith listings” that they know to be fictitious and fraudulent, thus forcing the Locksmiths to pay for advertising highlighted earlier in searches for “locksmith” and related terms. *Id.* at 8-9.

According to the complaint, scam locksmiths operate without required licensing, and they “usually lack the experience and specialized tools needed . . . tell[ing] the customer the problem is worse than expected and [then] tak[ing] some drastic, destructive action (like drilling out the caller’s lock).” *Id.* at 13. Exorbitant payment is often required. *Id.* Because “[l]ocation-based internet search . . . is the primary means by which prospective customers seek locksmith services,” these “[s]cam locksmiths publish hundreds or thousands of unique websites targeting nearly every heavily populated geographic location . . . around the country,” portraying themselves as locally-based businesses when they often actually operate via call-centers that dispatch mobile, non-licensed scam locksmiths. *Id.* at 12-13. In contrast, the Locksmiths allege that they are licensed and/or registered to perform their trade pursuant to the requirements of their respective jurisdictions. *Id.* at 3-8, 11-12. Because states publish public lists of licensed locksmiths and registered businesses, the Locksmiths allege that the Providers have actual knowledge of which locksmiths are scammers. *Id.* at 17-18.

---

<sup>1</sup> *But see* Compl. 8 (alleging that Google controls 70%, Microsoft controls 20%, and Yahoo controls 12% “of all organic internet search queries conducted in the United States.”).

The Locksmiths allege that the Providers not only re-publish information generated by the scam locksmith websites, but also “enhance those listings . . . by creating brand new original content not found on the original web sites.” *Id.* at 16. Specifically, the Providers’ “original content includes fictitious addresses, photos, map locations, and map pinpoints for scam locksmiths as well as driving directions to and from the fictitious locations.” *Id.* at 19. For example, “if a scam locksmith states that it is located in Falls Church, Virginia, but gives no location information, the search engine will create a map and arbitrarily place a pinpoint someplace in Falls Church. The map and pinpoints are created entirely by the search engine provider, not by ‘another.’” *Opp. to Defs.’ Mot. Dismiss 5 (Opp.)*.

By thus burying legitimate locksmiths under scam listings that appear legitimate and local, the Locksmiths allege that the Providers have caused “a large number of formerly viable locksmiths” to go “out of business entirely,” while the Plaintiffs themselves “have lost 30-60% of their gross revenue since 2009 in the specific business arena of outbound consumer service calls.” *Compl. 9*. And since the Providers not only list the scammers, but also allow scam locksmiths to themselves purchase advertising, the Locksmiths allege that the Providers pressure them to pay for expensive advertising. *Id.* at 30. If the Providers banned scam locksmiths from their search results, the licensed Locksmiths aver that they would likely appear among the first local results. *Id.* at 29.

Furthermore, the Locksmiths allege that the Providers collude in adopting this policy towards the scam locksmiths, thus abusing their monopoly power and restraining trade in violation of federal antitrust laws. *Id.* at 26-28. The Providers also allegedly violate the Lanham Act by making false representations pertaining to the scam locksmiths, and commit five violations of state law: fraud, tortious interference with an economic advantage, unfair

competition, breach of contract, and conspiracy. *Id.* at 28-37. The Locksmiths seek injunctions that would require the Providers to stop publishing the scam locksmiths' information in jurisdictions where licensing is required, as well as damages, attorney fees, and costs associated with the litigation. *Id.* at 37-38.

Baldino's originally filed this suit on its own behalf in December 2016. In January 2017, the Court granted leave to amend the complaint. The first amended complaint, currently operative, added 13 new locksmiths and the class action allegations. Microsoft successfully moved to stay the claims against it made by Baldino's and Joe East Enterprises pending a decision on the motion to dismiss, on the ground that contracts with those parties arguably required that all such claims be decided in arbitration. The Providers now jointly move to dismiss the remaining claims.

## II. LEGAL STANDARDS

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim crosses from conceivable to plausible when it contains factual allegations that, if proved, would 'allow the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.'" *Banneker Ventures, LLC v. Graham*, 798 F.3d 1119, 1129 (D.C. Cir. 2015) (alteration omitted) (quoting *Iqbal*, 556 U.S. at 678). In undertaking this inquiry, a court will "accept all the well-pleaded factual allegations of the complaint as true and draw all reasonable inferences from those allegations in the plaintiff's favor." *Id.*

### III. ANALYSIS

#### A. Immunity Under the Communications Decency Act<sup>2</sup>

“Preemption under the Communications Decency Act is an affirmative defense, but it can still support a motion to dismiss if the statute’s barrier to suit is evident from the face of the complaint.” *Klayman v. Zuckerberg*, 753 F.3d 1354, 1357 (D.C. Cir. 2014). The statute provides that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider” and that “[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.” 47 U.S.C. §§ 230(c)(1), (e)(3). Accordingly, the D.C. Circuit has held that:

The Communications Decency Act mandates dismissal if (i) [the Defendant] is a “provider or user of an interactive computer service,” (ii) the information for which [the Plaintiff] seeks to hold [the Defendant] liable was “information provided by another information content provider,” and (iii) the complaint seeks to hold [the Defendant] liable as the “publisher or speaker” of that information.

*Klayman*, 753 F.3d at 1357 (quoting 47 U.S.C. § 230(c)(1)). All three of these requirements are satisfied here.

The first and third prongs of *Klayman* are not in dispute. Each of the Defendants is a “provider . . . of an interactive computer service” because each is a quintessential example of an “information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet.” *See id.* at § 230(f)(2). The Locksmiths clearly seek to hold the

---

<sup>2</sup> Federal question jurisdiction exists under 28 U.S.C. § 1331, given the Locksmiths’ federal claims under the Sherman Antitrust Act and the Lanham Act. Compl. 7. The Defendants do not dispute personal jurisdiction, given the nature of their businesses in the District. *Id.* 7-8.

Providers liable as the “publisher or speaker” of the scam locksmiths’ information, since the gravamen of the complaint is that the Providers are injuring the Locksmiths by publishing scam locksmith information. Compl. ¶¶ 132 (Count I), 140 (Count II), 159 (Count III), 157 (Count IV), 164 (Count V), 172 (Count VII), 184-86 (Count VIII).

As for the second prong, I conclude that the Locksmiths are indeed seeking to hold the Providers liable for “information provided by another information content provider.” *See* 47 U.S.C. § 230(c)(1).

The statute defines an “information content provider” as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.” *Id.* at § 230(f)(3). The Locksmiths contend that the Providers are “responsible for the creation or development of some of the [scam locksmith] information that they publish.” Opp. 5. The Locksmiths specifically rely on the Providers’ alleged creation of mapping information: when a scam locksmith reports that it is in a certain city, the Providers provide an array of mapping information that supplements the scammer’s claim, including “fictitious addresses, photos, map locations, and map pinpoints for scam locksmiths as well as driving directions to and from the fictitious locations.” Compl. 19; Opp. 5-6. However, Baldino’s has made these same arguments before, Second Am. Compl. at ¶¶ 5, 32, *Baldino’s*, 88 F. Supp. 3d at 546, No. 14-cv-00636 (alleging that Google publishes “falsely placed map pinpoints”); Br. of App., *Baldino’s*, 624 F. App’x 81 (arguing that “Google is aiding and abetting a fraud by . . . providing an enhanced platform . . . now allowing pictures, reviews, and map locations with pinpoints, creating a picture of legitimacy for an illegal and fraudulent listing”), and the Fourth Circuit affirmed the district court’s conclusion that “[scam] locksmiths

... are solely responsible for making any faulty or misleading representations.” *Baldino’s*, 624 F. App’x at 82. A review of the CDA immunity jurisprudence confirms this conclusion.

“[A] website does not create or develop content when it merely provides a neutral means by which third parties can post information of their own independent choosing online.”

*Klayman*, 753 F.3d at 1358 (finding CDA immunity for Facebook regarding threats posted by the Third Palestinian Intifada). Even when a website’s “structure and design” is aimed at developing legal information based on the input of allegedly illegal content from elsewhere, the website creator cannot be considered the provider of the original information. *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 256-58 (4th Cir. 2009). In *Nemet*, the Fourth Circuit considered an allegation that Consumeraffairs.com had “developed” defamatory online comments regarding the automobiles sold by Nemet Chevrolet, because the “structure and design” of the relevant website “develop[ed] information related to class-action lawsuits.” *Id.* at 257. *Nemet* reasoned that because “there is nothing unlawful about developing this type of content,” *id.*, and the complaint “does not show, or even intimate” that the website was responsible for the defamatory content at issue, *id.* (quoting *Iqbal*, 556 U.S. at 683), it was not plausible or “even a likely possibility” that Consumeraffairs.com had provided the information at issue. *Id.* at 257-58.<sup>3</sup>

---

<sup>3</sup> In this vein, the Locksmiths attempt to rely on *Anthony v. Yahoo Inc.*, in which a district court concluded that the CDA did not shield Yahoo from allegations that two of its dating sites “create[d] . . . false and/or nonexistent profiles . . . to trick people . . . into joining the service,” and also convinced users to renew their subscription by “circulat[ing] profiles of actual, legitimate former subscribers whose subscriptions had expired, thus giving the misleading impression that these individuals are still available for dates.” 421 F. Supp. 2d 1257, 1259 (N.D. Cal. 2006); Opp. 7. As to the allegation of Yahoo-created profiles, *Anthony* concluded that “No case . . . has immunized a defendant from allegations that it created tortious content.” *Id.* at 1262-63 (emphasis in original). And even though “third parties created the[] [expired] profiles” that Yahoo allegedly represented as currently active, *Anthony* reasoned that “the CDA only



Both *Klayman* and *Nemet* distinguish the Ninth Circuit’s decision in *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008). *Klayman*, 753 F.3d. at 1358; *Nemet*, 591 F.3d at 257. In *Roommates.com*, the Ninth Circuit held that a housing website was not entitled to CDA immunity for its conduct in requiring new subscribers to “disclose [their] sex, sexual orientation and whether they will bring children to the household,” as well as their own preferences regarding those same three criteria, and then structuring results in the website based on that information. 521 F.3d at 1164-65. Here, unlike in *Roommates.com*, there is no allegation that the Providers require the scam locksmiths to provide the allegedly fraudulent information at issue, or that the Providers have created a stand-alone platform for the provision of services.

However, the Ninth Circuit’s logic is nonetheless helpful. *Roommates.com* emphasized that “providing neutral tools to carry out what may be unlawful or illicit searches does not amount to ‘development’ for purposes of the immunity exception.” 521 F.3d at 1169. “If an individual uses an ordinary search engine to query for a ‘white roommate,’” the Ninth Circuit reasoned, “the search engine has not contributed to any alleged unlawfulness in the individual’s conduct.” *Id.* The court also explained that the same reasoning governed *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003)—in which a prankster created a fake, libelous dating profile for an actress—because “the website provided neutral tools, which the

---

entitles Yahoo! not to be ‘the publisher or speaker’ of the profiles. It does not absolve Yahoo! from liability for any accompanying misrepresentations. Because *Anthony* posits that Yahoo!’s manner of presenting the profiles—not the underlying profiles themselves—constitute fraud, the CDA does not apply.” *Id.* at 1263. The instant case is not controlled by the logic of *Anthony*. Although the Locksmiths do allege that the Providers create the mapping information, it is the scam locksmiths’ underlying location claim that is allegedly false; no “accompanying misrepresentations” are adequately plead. Moreover, in *Anthony*, Yahoo was acting as a host and creator of proprietary dating sites, quite unlike the generic search aggregation function that is at issue here.

anonymous dastard used to publish the libel, but the website did absolutely nothing to encourage the posting of defamatory content—indeed, the defamatory posting was contrary to the website’s express policies.” *Id.* at 1171. The same reasoning applies here, where the Providers’ offer neutral mapping functionality with no encouragement for websites to provide false or misleading location claims. The fact that scam locksmiths make use of these neutral mapping tools does not constitute “development” of the underlying location claims by the Providers, for purposes of the CDA.

Under the logic of *Roommates.com*, the “development” of content is “not merely . . . augmenting the content generally, but . . . materially contributing to its alleged unlawfulness.” *Roommates.Com*, 521 F.3d at 1167–68; *see also Jones v. Dirty World Entm’t Recordings LLC*, 755 F.3d 398, 410 (6th Cir. 2014) (citing *Roommates.Com* as the “leading” circuit decision providing a “workable” definition of information “development.”). To the extent that the Locksmiths press this argument, I conclude that the Providers’ mapping information does not materially contribute to the alleged unlawfulness of the underlying information. As the Sixth Circuit reasoned in *O’Kroley v. Fastcase, Inc.*, the CDA immunizes a search engine’s “automated editorial acts.” 831 F.3d 352, 355 (6th Cir. 2016). When a search engine re-publishes information originally created by a third party, CDA immunity applies even when confusion may result. *Id.* Here, it is the scam locksmiths who provide the original location claim, and the Providers have created a website that simply re-publishes that information along with associated mapping information. The extra information is wholly dependent on the original location claim, and does not materially contribute to the alleged unlawfulness of the original claim. After all, the Locksmiths do not even allege that the Providers should ban those who make false location claims. Compl. 17-18. It is the scam locksmiths’ *unlicensed status* that

Plaintiffs claim should prompt a ban, and they infer from this fact that “we’re a local business” claims are questionable.<sup>4</sup> In short, the maps are essentially unrelated to any unlawful conduct.

In common sense terms, it is the scam locksmiths and not the Providers who are providing the information that potentially creates liability here. The complaint strains to avoid this conclusion, alleging that the mapping information “independently and deliberately deceives consumers beyond the original deception purveyed by the scam locksmiths,” and “facilitate[s], enhance[s], and legitimize[s]” the scam locksmiths. Compl. 19-20. But most websites that incorporate content from elsewhere could be said to “facilitate, enhance, and legitimize” original content by amplifying its reach or improving its relevance and presentation. By presenting Internet search results to users in a relevant manner, Google, Yahoo, and Microsoft facilitate the operations of every website on the internet. The CDA was enacted precisely to prevent these types of interactions from creating civil liability for the Providers.<sup>5</sup> The fundamental legal question is whether the Defendants “provided” the specific information for which Plaintiffs seek to hold them liable. The gravamen of this complaint is *precisely* that the Providers are financially liable for re-publishing the scam locksmiths’ information. Accordingly, I conclude that the Locksmiths seek to hold the Providers liable for “information provided by another

---

<sup>4</sup> See, e.g. Compl. 12 (“Scam locksmiths’ websites . . . include false claims that they are local businesses with local phone numbers. They do this deliberately, to misrepresent themselves to consumers as nearby businesses. When a user calls the local-area phone number for the scam locksmith, he or she may be put through to a call center, in another city or even another country. An operator sends over a putative ‘locksmith’ on behalf of the scam company.”)

<sup>5</sup> The result might be different if a plaintiff alleged that the Providers used outdated maps in violation of some duty of care, or intentionally navigated users across dangerous roads. But that is not the case. The maps are objectionable because of the underlying information the scam locksmiths supply, and for no other reason.

information content provider,” satisfying the CDA’s second requirement. *See* 47 U.S.C. § 230(c)(1).

Furthermore, none of the CDA’s exceptions apply here, as the Locksmiths concede. Tr. of Proceedings 10; Opp. 3-7 (never mentioning a statutory exception). One exception requires that “[n]othing in [Section 230] shall be construed to impair the enforcement of . . . any . . . Federal criminal statute.” 47 U.S.C. § 230(e)(1). Although the Plaintiffs do plead criminal violations of the federal antitrust laws, the exception “is limited to criminal prosecutions” and “excludes civil suits.” *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 23 (1st Cir. 2016). The CDA also has “no effect” on intellectual property law, consistent state laws, or “the Electronic Communications Privacy Act . . . or any similar State law.” 47 U.S.C. § 230 (e)(2)-(4). However, none of the Locksmiths’ claims implicate these subject matters. *See* Defs.’ Mot. Dismiss 7-8 (addressing each exception).

Accordingly, all of the Locksmiths’ claims are barred by CDA immunity, except for the breach of contract claim in Count VI.

## **B. Breach of Contract**

The Locksmiths also sue for breach of contract, claiming a violation of the “implied duty of good faith and fair dealing.” Compl. 32-33. The amended complaint inconsistently alleges that both one and many plaintiffs have “contracted some of listed defendants for paid advertising services,” but none of the actual contract(s) are provided. *See* Compl. 22, 32.

The Providers argue that because the complaint does not identify what particular contracts exist, it therefore fails to put them on notice of the basis for the claim. Defs.’ Mot. Dismiss 17. They rely on *Bissessur v. Indiana Univ. Bd. of Trustees*, a Seventh Circuit case that dismissed an implied contract claim in which the plaintiff argued “that the exact details of the

contract will become clear during discovery.” 581 F.3d 599, 603 (7th Cir. 2009). *Bissessur* rejected this ‘find-the-contract-in-discovery’ argument, relying on the Supreme Court’s decision in *Twombly*, and the recognition that “[o]ur system operates on a notice pleading standard.” *Id.*

The court reasoned:

[I]t is not enough to give a threadbare recitation of the elements of a claim without factual support. A plaintiff may not escape dismissal on a contract claim, for example, by stating that he had a contract with the defendant, gave the defendant consideration, and the defendant breached the contract. What was the contract? The promises made? The consideration? The nature of the breach?

*Id.* Here, I am reasonably confident that contracts existed between at least two of the 14 locksmiths (Baldino’s and Joe East Enterprises) and Microsoft, since those parties consented to a stay pending potential arbitration based on the contracts’ existence. But those claims are precisely the ones *not* before the Court on this motion to dismiss, and no other specific contracts have been alleged.

Although other contracts very well may exist, Plaintiffs have not provided sufficient “factual content” to allow me to “draw the reasonable inference that the defendant is liable.” *See Iqbal*, 556 U.S. at 678. Even if I inferred that Defendants’ conduct would violate contractual duties if a contract existed, I cannot reasonably infer which Defendants are liable to which Plaintiffs, without any information about the existence of specific contracts. Accordingly, Count VI must be dismissed as well.

#### **IV. CONCLUSION**

For the aforementioned reasons, the Defendants’ Motion to Dismiss is GRANTED. Pursuant to the Court’s decision on CDA immunity, Counts I-V and VII-VIII are dismissed with

prejudice. The breach of contract claim, Count VI, is dismissed without prejudice. A separate order will issue.

Dated: January 11, 2018

/s/  
TREVOR N. MCFADDEN  
United States District Judge